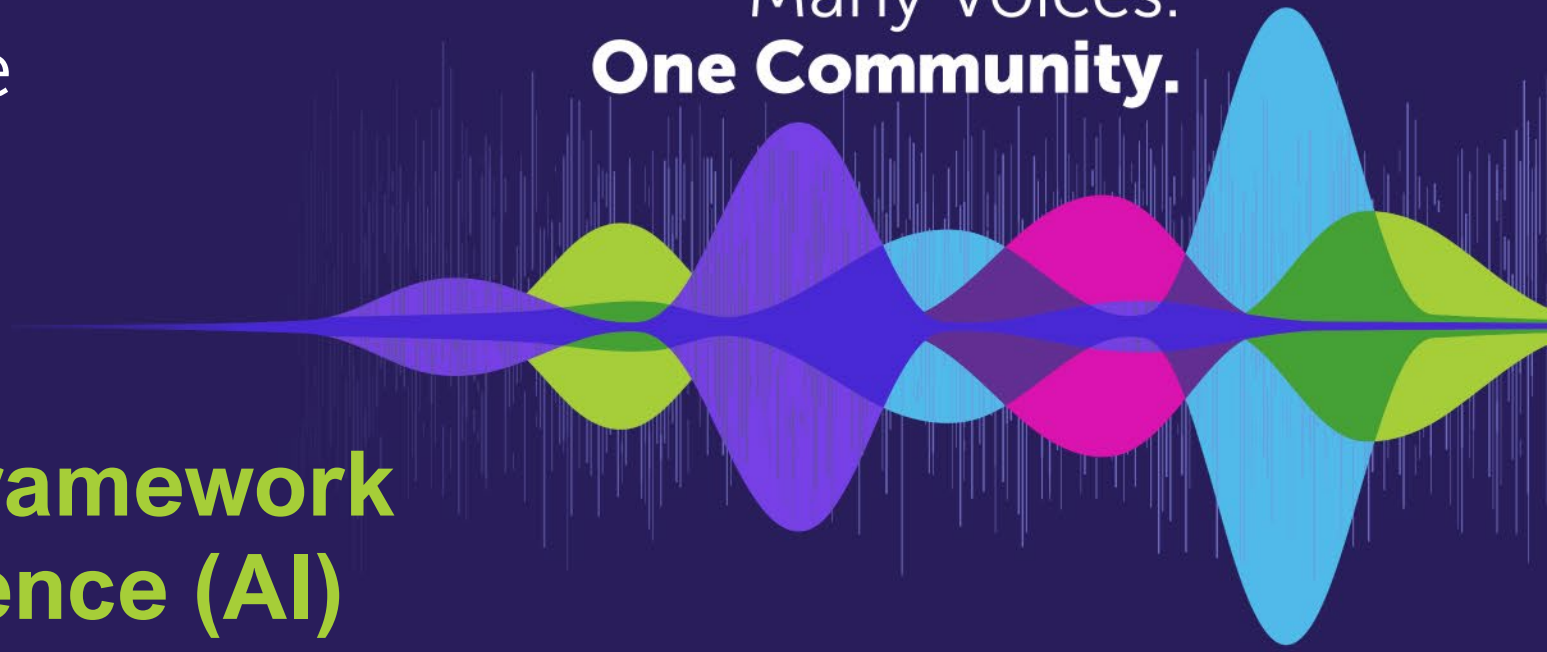
RSAC 2025 Conference

Many Voices. One Community.

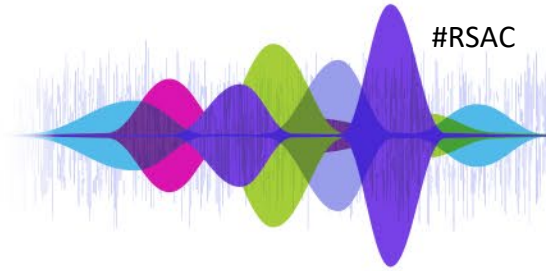


SESSION ID: SAT-M01

The Cybersecurity Framework and Artificial Intelligence (AI)

Katerina Megas
Program Manager
NIST
https://www.linkedin.com/in/kmegas/

Julie Snyder
Principal, NCF Community Profiles & Privacy Lead
MITRE
https://www.linkedin.com/in/julienetherysnyder/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Speakers

Katerina Megas

NIST

https://www.linkedin.com/in/kmegas/

Julie Snyder

MITRE

https://www.linkedin.com/in/julienetherysnyder/

RSAC 2025 Conference

The Challenges

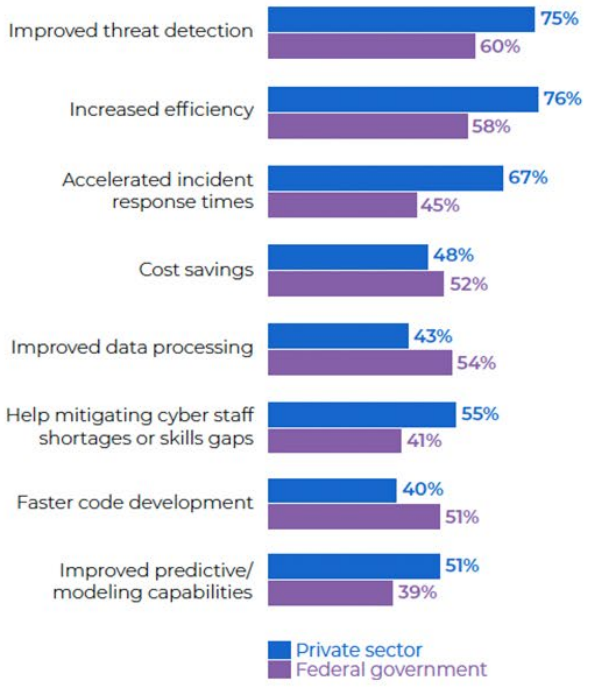
AI is Widely Used Across Critical Infrastructure

- Event Detection
- Incident Response
- Modeling & Simulation
- Physical Security
- Automation of Operations
- Systems Planning
- Operational Awareness
- Forecasting
- Performance Optimization
- Research & Development (R&D)
- Customer Service Automation

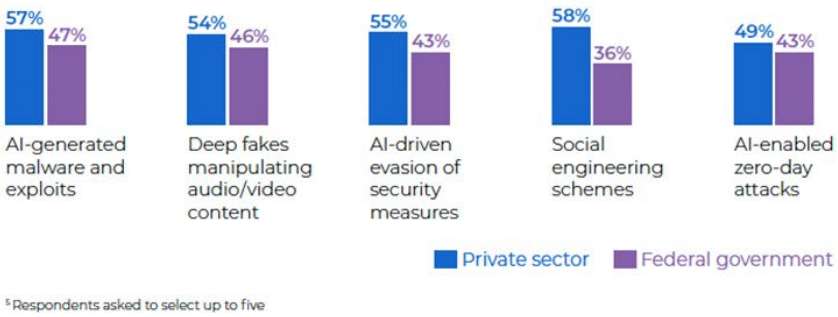
AI-enabled Cybersecurity is Growing, With Challenges

"One in three cybersecurity leaders (31%) say their organization is using AI for cyber today"

What benefits do you see for incorporating AI into cybersecurity practices?[1]



Which of the following AI-driven attack strategies do you think pose the greatest threats to your organization?[5]



[5] Respondents asked to select up to five

80% of cyber leaders say accelerating AI adoption is critical to their organization's resilience against evolving threats

What challenges, if any, are having the biggest impact on your organization's adoption of AI for cybersecurity?[5]

#1 Fears of increased attacks on new AI models, data, or services

"We have to teach our CEOs and CIOs to change their language. Instead of saying, 'Is it ready yet?' or 'Is it running?' ... the question needs to be, '**Is it resilient?**'"

– Private sector cyber leader

#2 Lack of skilled workforce to implement

"The number of people that are skilled in both cybersecurity and machine learning is **extremely small** right now."

– Private sector cyber leader

#3 Data quality, integrity, or availability challenges

"Never fully trust the data lakes you are getting information from; always complete a **thorough review** process."

– Private sector cyber leader

- The Art of Human and AI Teaming in Cybersecurity (https://meritalk.com/download-pdf/?from=188933)

The State of AI Cybersecurity in 2025 and Beyond

The State Of AI Cybersecurity In 2025 And Beyond

Forbes

Rohan Pinto Forbes Councils Member
Forbes Technology Council COUNCIL POST |

Rohan Pinto is CTO/Founder of 1Kosmos Block
technologist with a strategic vision to lead tech
initiatives.

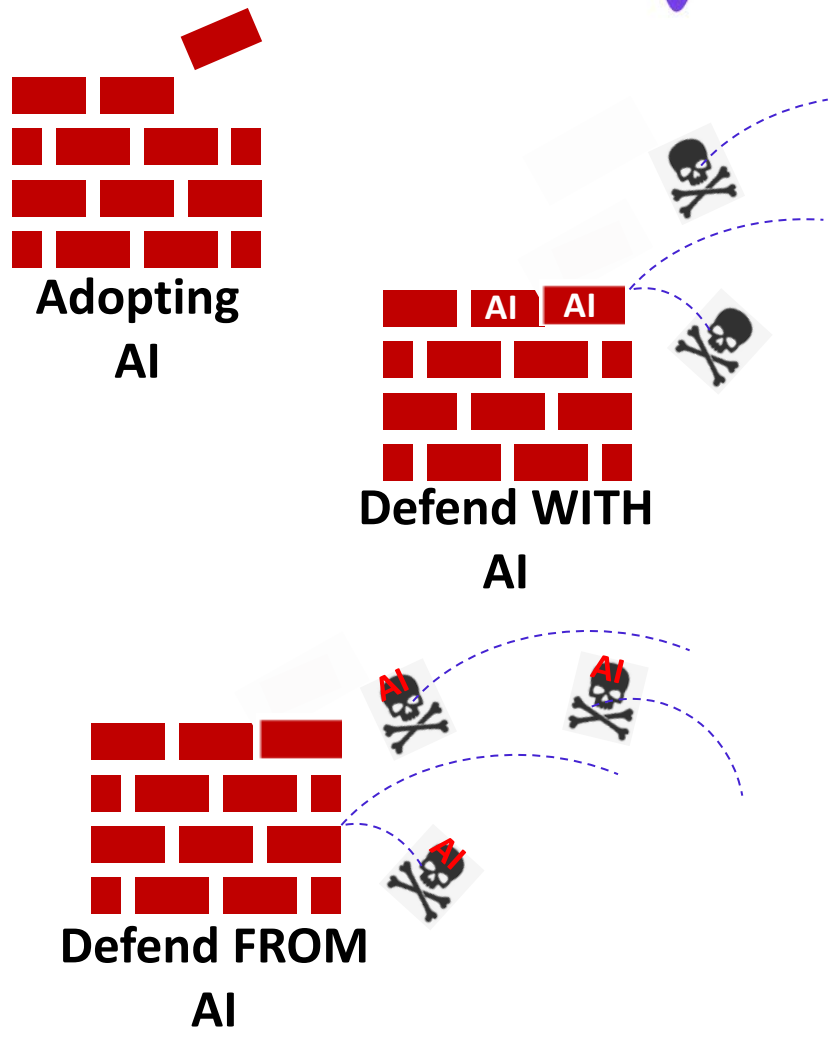
GETTY

"The year 2025 represents a watershed moment in the history of cybersecurity, as the convergence of artificial intelligence (AI), advanced persistent threats and increasingly complex digital ecosystems reshape the landscape. AI, which was originally solely used for automation and optimization, now acts as both a shield and a sword in the field of cybersecurity. This article delves into the state of AI in cybersecurity as of 2025, including rising trends and future issues."

The State Of AI Cybersecurity In 2025 And Beyond
Forbes
January 21, 2025

Challenges and Concerns We Are Hearing from the Cyber Community

1. CISO's are concerned with how to strategically address the emerging cybersecurity risks stemming from advancements in AI but their hands are already full dealing with current ongoing operations and they could benefit from prioritization
2. There is already much ongoing discussion and work in many of these areas but there is no consistent taxonomy or relation to an organizations strategic cybersecurity risk management
3. There are some new or modified impacts to cybersecurity but do not reinvent the wheel, rather build on existing frameworks or cybersecurity practices and identify the what is new
4. There is limited overlap between cybersecurity practitioner/training and AI practitioner/training
5. AI and cybersecurity practitioners play differing roles in risk management and use differing terminology



Examples of New or Modified AI-related Cyber Risks

Protection of AI Systems

Adopting AI can create new risks and expand attack surface

- Manipulation of AI algorithms, data, or sensors
- Injection of prompts into an AI system that cause system malfunction or the disclosure of sensitive information

AI-enabled Cyber Operations

Defend against AI-facilitated cyberattacks from adversaries

- Augment threat actor capabilities and operations (e.g., scale cyberattacks)
- Collect and analyze data to identify and monitor targets for potential attacks
- Psychological manipulation to trick users into revealing sensitive information or performing actions that compromise security controls, including the use of deepfakes or AI-enhanced phishing attempts

AI can be used to enhance and scale cyber defense

- Augment existing capabilities to detect, prevent, and respond to cyberattacks
- Augment protection of network infrastructure from unauthorized access, misuse, or theft

Examples:

- autonomous malware
- reconnaissance
- use of deepfakes
- automatic parsing of text for vulnerability insights
- modeling and model inference and completion
- unauthorized data access
- cyberattack detection evasion
- vulnerability identification and exploitation
- machine-speed decision-making, optimization, prompt injections to reveal sensitive information

RSAC™ 2025 Conference

The Case for a Cyber AI Profile

The Case for a Cyber AI Profile

Purpose:

Support cybersecurity programs as they manage the impacts of advancements in AI to their organization

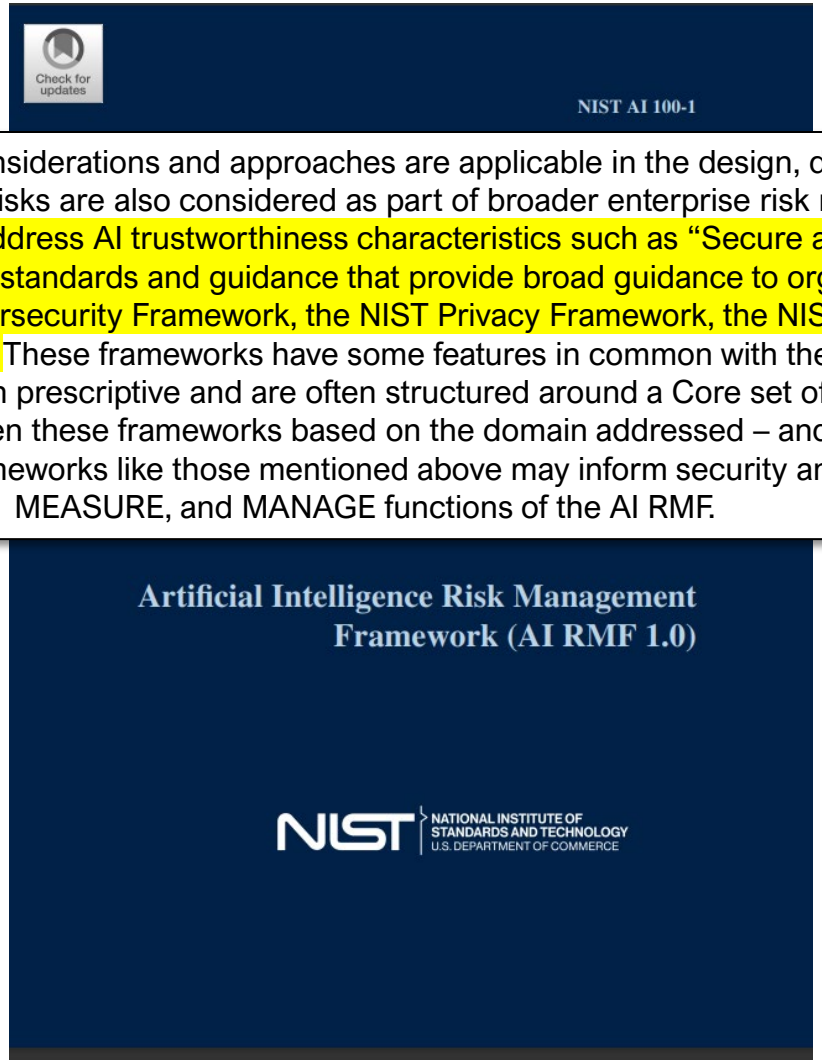
Areas of focus:

- Cybersecurity risks that arise from the use of AI by organizations, including securing AI systems, components, and machine learning infrastructures, and minimizing data leakage.
- Determining how to defend against AI-enabled attacks.
- Assisting organizations in the use of AI with their cyber defense activities and using AI to improve privacy protections.

Outcomes:

- Establishes a shared understanding of AI-related cybersecurity priorities and considerations for any organization
- Fosters collaboration and communication across the AI and cybersecurity communities
- Enables organizations that are using AI technologies to demonstrate a degree of commitment and trustworthiness using a common set of outcomes in the Profile

The AI RMF Points to the CSF for Managing Cybersecurity Risk


Check for updates
NIST AI 100-1
Artificial Intelligence Risk Management Framework (AI RMF 1.0)
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

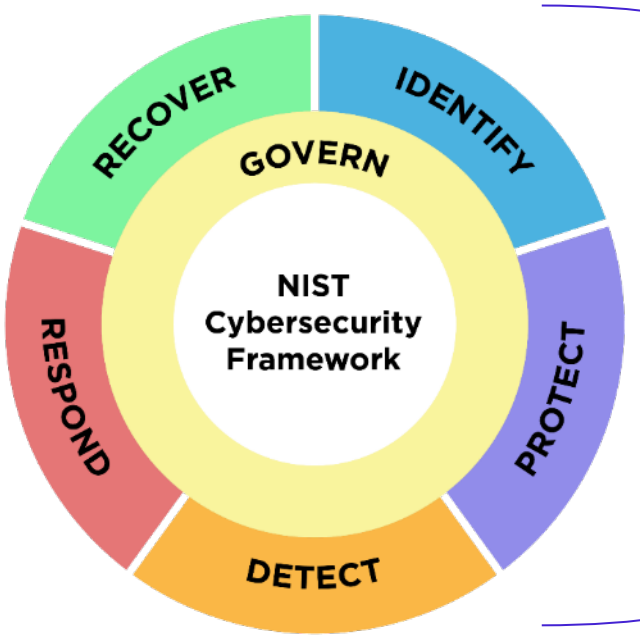
Privacy and cybersecurity risk management considerations and approaches are applicable in the design, development, deployment, evaluation, and use of AI systems. Privacy and cybersecurity risks are also considered as part of broader enterprise risk management considerations, which may incorporate AI risks. As part of the effort to address AI trustworthiness characteristics such as "Secure and Resilient" and "Privacy-Enhanced," organizations may consider leveraging available standards and guidance that provide broad guidance to organizations to reduce security and privacy risks, such as, but not limited to, the NIST Cybersecurity Framework, the NIST Privacy Framework, the NIST Risk Management Framework, and the Secure Software Development Framework. These frameworks have some features in common with the AI RMF. Like most risk management approaches, they are outcome-based rather than prescriptive and are often structured around a Core set of functions, categories, and subcategories. While there are significant differences between these frameworks based on the domain addressed – and because AI risk management calls for addressing many other types of risks – frameworks like those mentioned above may inform security and privacy considerations in the MAP, MEASURE, and MANAGE functions of the AI RMF.

About CSF 2.0

NIST has updated the widely used Cybersecurity Framework (CSF)—its landmark guidance document for reducing cybersecurity risk.

The Framework is comprised of:

- **CSF Core**
- **CSF Organizational Profiles**
- **CSF Tiers**



Together, these six Functions provide a comprehensive view for managing cybersecurity risk.

CSF 2.0 Profiles

Framework Profiles

Provide a way to understand, tailor, assess, prioritize, and communicate the Core's outcomes based on mission objectives, stakeholder expectations, threat landscape, and requirements.

Organizational Profiles

Describes an organization's current and/or target cybersecurity posture in terms of the Core's outcomes

Community Profiles

Describes CSF outcomes to address shared interests and goals among multiple organizations

Community Profiles facilitate CSF implementation and help each community address its specific cybersecurity challenges.

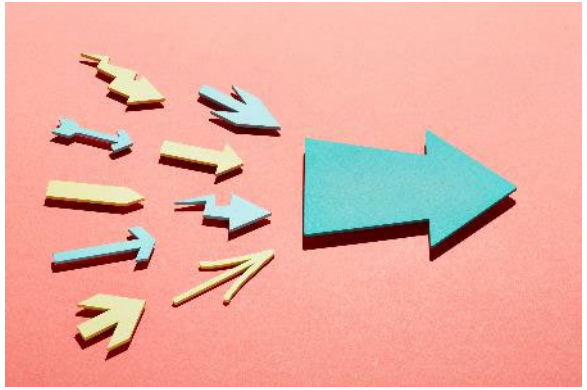
What could be in a Cyber AI Profile?

The outcomes described in the NIST Cybersecurity Framework (CSF) 2.0 provide a practical way to help organizations understand, examine, and address the cybersecurity risks introduced by the adoption of AI.

Common Priorities

AI-specific Cybersecurity Implications

Illustrative Examples and Informative References



Mappings to Other NIST Frameworks

RSAC 2025 Conference

About Community Profiles

Communities

Organizations that share a common context and an interest in their cybersecurity posture:

- **Sectors/subsectors (e.g., critical infrastructure sectors)**
- **Technologies (e.g., AI, mobile, cloud)**
- **Other use cases**

Benefits of Community Profiles

Use **shared taxonomy** for cybersecurity and privacy in the context of the community

Align requirements from multiple sources

Leverage expertise across the community

Encourage **common target** outcomes

Minimize the burden by working together

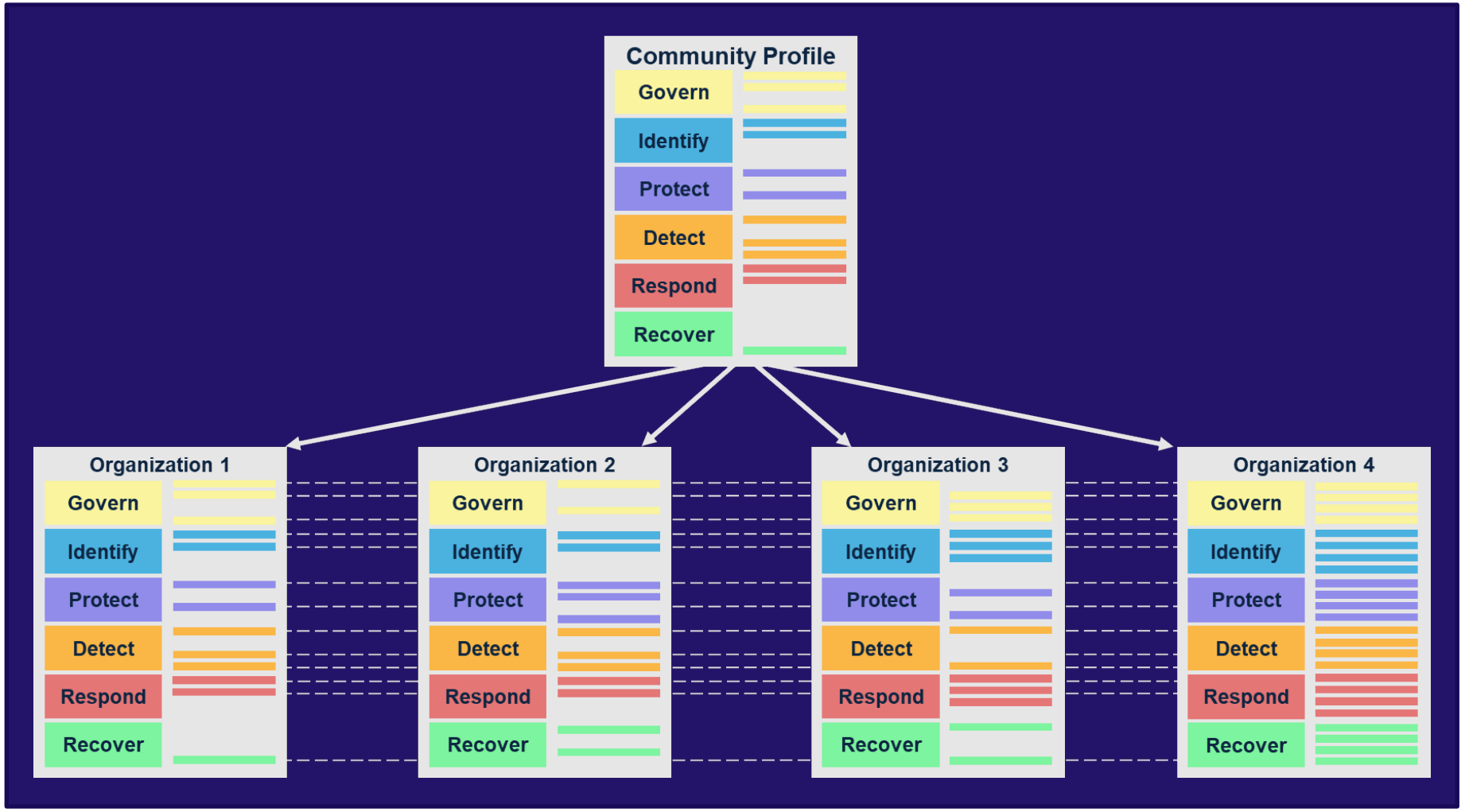
Communicate about cybersecurity and privacy risk

Source (adapted): *Pascoe C, Snyder JN, Scarfone KA (2024) NIST Cybersecurity Framework 2.0: A Guide to Creating Community Profiles. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 32 ipd. https://doi.org/10.6028/NIST.CSWP.32.ipd*

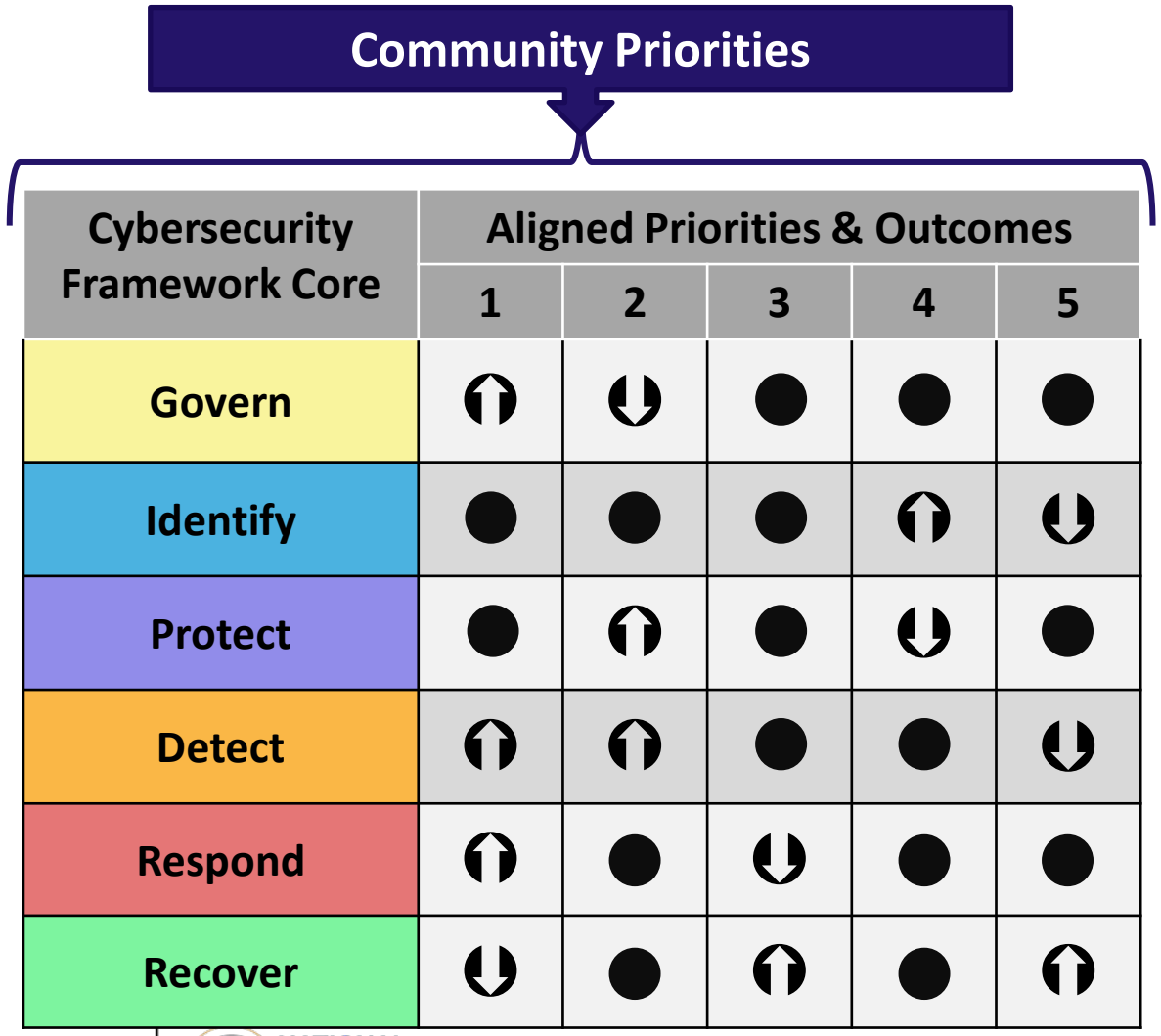
Community Profile Content

A Community Profile offers a common view.

Organizations can describe where and why they deviate from the Community Profile and each other and engage in risk discussions with a common starting point.



Community Profiles Inform Organizational Target Profiles



Notional Priority Levels*:

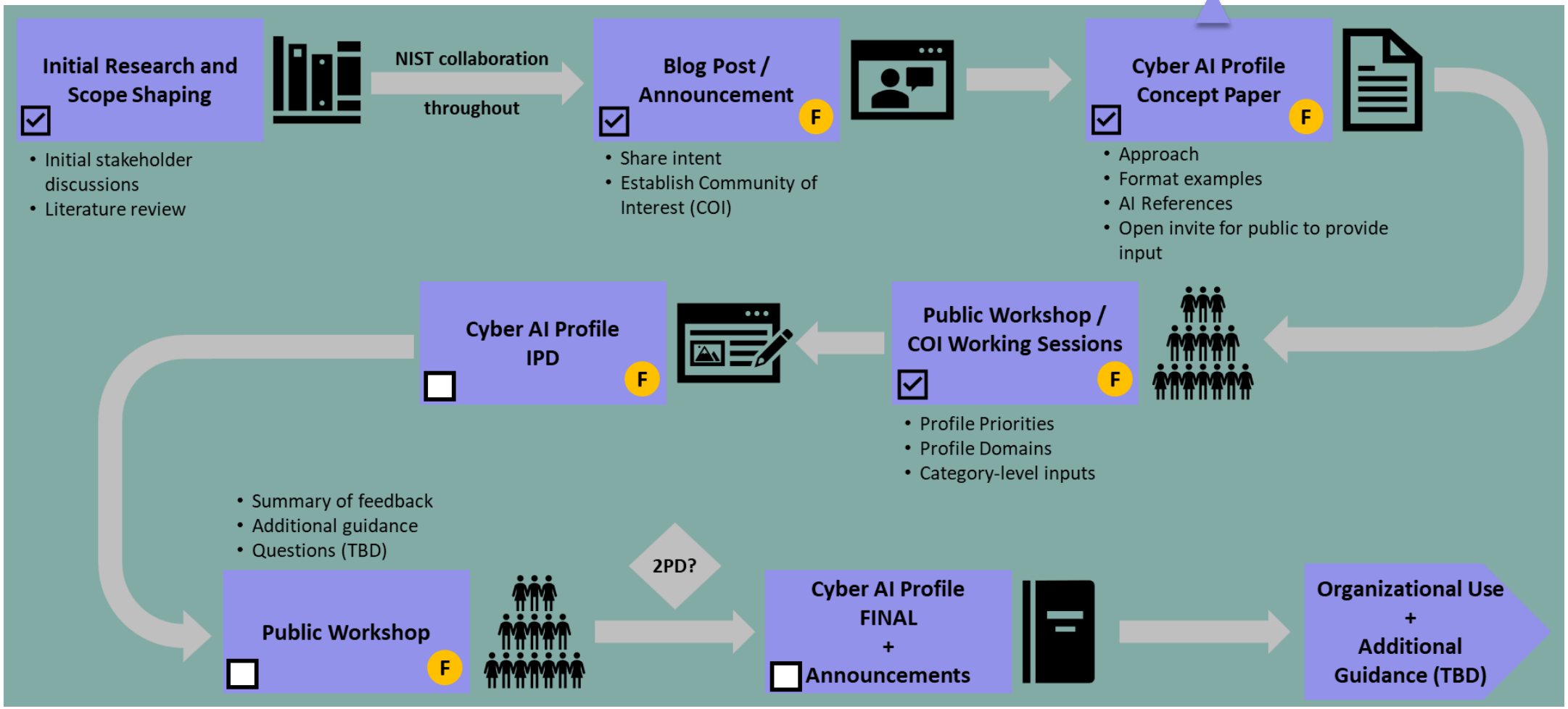
- ↑ Higher
- ● Same as Community Profile
- ↓ Lower

*Communities and organizations can choose any prioritization schema that works best for them

RSAC 2025 Conference

Creating the Cyber AI Profile

Cyber AI Profile Roadmap



F Opportunities for COI/public stakeholder feedback (NOTE: Internal NIST collaboration occurs throughout)

Questions we asked the Community

Scope:

- Is it appropriate to develop or modify existing cybersecurity-focused guidelines and resources to specifically address how AI advances change cybersecurity risks and opportunities?
- Is it appropriate to separately develop or modify existing AI-focused risk management guidelines and resources to specifically address cybersecurity considerations?
- Are we focusing on the right areas (securing AI system components, thwarting AI-enabled attacks, and leveraging AI in organizations' cybersecurity approaches)?
- Are there any key areas missing that are at the intersection of cybersecurity and AI?
- Should AI design and implementation failures be included?

Cybersecurity Risks:

- What existing NIST guidance or best practices should be included to address the needs of various stakeholders?
- What gaps in NIST guidance exist that should be filled?

Multi-dimensional Views:

- Should NIST expand this effort to include demonstrating the relationship between cybersecurity and privacy of AI?
- In what ways might NIST better represent the relationship across its cybersecurity, privacy, and AI resources?

Related Efforts:

- What groups and activities should we connect with to inform our efforts?
- Are there emerging standards activities we should consider? If so, which ones?

Other Considerations:

- What else should we consider to inform the development of meaningful guidance in these areas?

What could be in a Cyber AI Profile?

Provide guidance to support cybersecurity programs as they manage the impacts of advancements in AI to their organization

- Identify the common priority areas they are most concerned with based on input from the community
- Organize the discussion of these cybersecurity implications around the Functions, Categories, and Subcategories of the CSF Core
- Illustrative examples and Informative References useful to organizations

Example #1:

Awareness and Training (PR.AT) With advancements in the use of AI by cyber adversaries, organizations may need to consider revising their employee training (PR.AT-01) to raise awareness of AI-enabled spear phishing methods or other social engineering attacks. An organization may need to add new training for staff in specialized cybersecurity roles (PR.AT-02) as the organization adopts AI technologies.

Example #2:

Risk Assessment (ID.RA) AI technologies are used by our adversaries to become faster and more efficient at exploiting a vulnerability from the time it is discovered. Organizations may need to revisit their current processes for how they identify vulnerabilities (ID.RA-01) or for responding to vulnerability disclosures (ID.RA-08).

Example #3:

Asset Management (ID.AM) As AI technologies are adopted and given the new attack surface and ways that AI systems may be exploited, organizations may need to revise their current approach to identifying their data assets (ID.AM-02) or how their data is managed

What could be in a Cyber AI Profile?

CSF Core	Securing AI System Components	Thwarting AI-enabled Cyber Attacks	Conducting AI-enabled Cyber Defense	Informative References / Mappings
CSF.XX-01: [Subcategory text]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[Pointers to related, laws, regulations, guidance, mappings, etc.]
CSF.XX-02: [Subcategory text]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[Pointers to related, laws, regulations, guidance, mappings, etc.]
CSF.XX-03: [Subcategory text]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[AI-specific implications and considerations for achieving this cybersecurity outcome.]	[Pointers to related, laws, regulations, guidance, mappings, etc.]

Preliminary feedback so far

- Broad **support for the approach** discussed in the concept paper
  - Three focus areas
  - Starting with CSF 2.0
- AI is benefiting **both the defender and the attackers**
- **Existing frameworks should be extended** to address AI-specific risks
  - Don't re-invent wheel
  - Interest in mapping concepts between frameworks (CSF, Privacy, and AI RMF)
  - Similar need based on RMF SP 800-53
  - Some feedback calling for integrating the AI RMF
- **Data is the Crown Jewel**—and the weakest link, consider data in the scope of securing AI
- **AI supply chain security** is the next big battleground
- Other issues on peoples' minds:
  - Human-in-the-loop
  - **Agentic AI**
  - **Governance frameworks** to ensure AI solutions adhere to security best practices and compliance mandates.
- **Practical guidance** on implementing the Cyber AI Profile, including training, tools, and resources.
- Differentiate between AI-augmented and AI-native attacks

RSAC™ 2025 Conference

Next Steps

Many Voices.
One Community.

Apply What You Have Learned Today

- Next week you should:
  - Join the Cyber AI Profile Community of Interest
  - Review the Cybersecurity and AI Workshop Concept Paper and recent workshop materials
  - Visit the NIST NCCoE Frameworks Resources page to learn more about Community Profiles
- In the first three months following this presentation you should:
  - Plan to participate in the public comment process for the the Cyber AI Profile Initial Public Draft (ipd)
  - Begin thinking about how your organization can use the Cyber AI Profile
- Within six months you should:
  - Continue providing inputs to NIST for the Cyber AI Profile and other resources
  - Start using the Cyber AI Profile (once final)

How to Engage

Please follow our project and join the Community of Interest to stay tuned regarding our progress and opportunities to get involved!

https://www.nccoe.nist.gov/projects/csf-20-ai-profile

Cyber AI Profile Workshop – April 2025

NIST Cybersecurity Framework

NIST AI Risk Management Framework

Cybersecurity and AI Workshop Concept Paper

RSAC 2025 Conference

Many Voices. One Community.

Thank you!

Kat Megas

Julie Snyder

Contact us: cyberAIprofile@nist.gov